

SOME REMARKS ON COVERINGS OF THE PROJECTIVE LINE OVER FINITE FIELDS

CRISTINA MARTÍNEZ AND ALBERTO BESANA

ABSTRACT. We study finite Galois extensions of the rational function field of the projective line $\mathbb{P}^1(\mathbb{F}_q)$ over a finite field \mathbb{F}_q of q elements defined by considering quotient curves by finite subgroups of the projective linear group $PGL(2, q)$, and we enumerate them expressing the count in terms of Stirling numbers.

1. INTRODUCTION

Let denote by \mathbb{F}_p the Galois field of p elements. Any other field F of characteristic p contains a copy of \mathbb{F}_p . Any $V = \mathbb{F}_p^n$ field extension of \mathbb{F}_p is a \mathbb{F}_p vector space and a $n - 1$ dimensional projective space $\mathbb{P}^{n-1}(\mathbb{F}_p)$.

The multiplication map $m_y : \mathbb{F}_p^* \rightarrow \mathbb{F}_p^*$, mapping $x \mapsto yx$ is \mathbb{F}_{p^2} -linear and induces an automorphism of the projective plane $\mathbb{P}^2(\mathbb{F}_{p^2})$ of order p^2 .

Two points $x = (x_0, x_1, x_2)$ and $y = (y_0, y_1, y_2) \in \mathbb{F}_{p^3}$ are equivalent if and only if $y_i = t x_i$ for $i \in \{0, 1, 2\}$, for some $t \in \mathbb{F}_p^*$. Therefore the number of points in $\mathbb{P}^2(\mathbb{F}_p)$ is $\frac{p^3-1}{p-1} = p^2 + p + 1$ and dually there are $p^2 + p + 1$ lines in $\mathbb{P}^2(\mathbb{F}_p)$. There are $p + 1$ points on every line and $p + 1$ lines through every point. By induction on n , we easily see that the number of points in $\mathbb{P}^n(\mathbb{F}_p)$ is $p^n + p^{n-1} + \dots + p + 1$.

In the present note, we study genus g projective plane algebraic curves that are d sheeted coverings of \mathbb{P}^1 and we count them over \mathbb{F}_p . Each isomorphism class over \mathbb{F}_p is counted with the reciprocal of the number of \mathbb{F}_p -automorphisms.

Definition 1.1. *Given a polynomial $f \in \mathbb{F}_p[x, y, z]$, the curve $\mathcal{C}_f = V(f)$ defined on $\mathbb{P}^2(\mathbb{F}_p)$ is nonsingular. More precisely $V(f)$ is the set of rational points of the curve \mathcal{C} and f is the ideal generated by f in $\mathbb{F}_p[x, y, z]$. The degree d of the curve is the degree of its polynomial.*

Let us denote by F the function field of the curve \mathcal{C}_f and by $\mathbb{P}(F)$ the set of places of F . For $P \in \mathbb{P}(F)$ we denote by \mathcal{O}_P the valuation ring of P , and by ν_P the discrete valuation induced by P in F . The set of places $\mathbb{P}_1(F)$ of F of degree one are called rational places of F , i.e. $N(F) = |\mathbb{P}_1(F)|$. In the present paper, we will concentrate in curves that are coverings of the projective line $\mathbb{P}^1(\mathbb{F}_q)$ where q is a power of a prime p . Moreover in Theorem 2.7, we characterize all coverings of $\mathbb{P}^1(\mathbb{F}_q)$ by projecting its automorphism group to the known finite subgroups of $PGL(2, q)$ the automorphism group of the rational function field.

2000 *Mathematics Subject Classification.* 11T55 (primary) ; 11T71 (secondary) .

Key words and phrases. Algebraic curve, covering, finite fields, Stirling number.

2. KUMMER EXTENSIONS OF THE RATIONAL FUNCTION FIELD

From now \mathbb{F}_q will be a field with $q = p^n$ elements and \mathcal{C} a non-singular, projective, irreducible curve defined over \mathbb{F}_q , defined by the vanishing locus of a polynomial $F \in \mathbb{F}_q[x_0, x_1, x_2]$. We define the number N of \mathbb{F}_q -rational points on the curve to be

$$N = |\{(x_0, x_1, x_2) \in \mathbb{P}^2(\mathbb{F}_q) | F(x_0, x_1, x_2) = 0\}|.$$

The number of points $\overline{\mathcal{C}}(\mathbb{F}_{q^r})$ on \mathcal{C} over the extensions \mathbb{F}_{q^r} of \mathbb{F}_q is encoded in an exponential generating series, called the zeta function of $\overline{\mathcal{C}}$:

$$Z(q, t) = \exp \left(\sum_{r=1}^{\infty} \# \overline{\mathcal{C}}(\mathbb{F}_{q^r}) \frac{t^r}{r} \right).$$

Theorem 2.1. *The number of \mathbb{F}_q rational points of a nonsingular plane curve \mathcal{C} of genus g and degree d satisfies the following bounds:*

- (1) (Hasse-Weil bound) $N \leq q + 1 + 2g\sqrt{q}$;
- (2) (Stöhr-Voloch bound) $N \leq \frac{1}{2}(2g - 2 + (q + 2)d)$.
- (3) (Weil) $\mathcal{C}(\mathbb{F}_{q^2}) \leq 1 + q^2 + 2qg$.

The curve \mathcal{C} is called \mathbb{F}_{q^2} -maximal if it attains the upper bound above; i.e. if one has

$$\# \mathcal{C}(\mathbb{F}_{q^2}) = 1 + q^2 + 2q \cdot g.$$

The most well-known example of a \mathbb{F}_{q^2} -maximal curve is the so called hermitian curve \mathcal{H} , which can be given by the plane model:

$$x^{q+1} + y^{q+1} + z^{q+1} = 0.$$

Thus many examples of \mathbb{F}_{q^2} -maximal curves arise by considering quotient curves \mathcal{H}/G , where G is a subgroup of the automorphism group of \mathcal{H} .

Lemma 2.2. *Any finite Galois extension $F = \mathbb{F}_p(t) \hookrightarrow F'$ correspond to a Galois covering $C \rightarrow \mathbb{P}^1(\mathbb{F}_p)$ with $\text{Gal}(C/\mathbb{P}^1(\mathbb{F}_p)) = \mathbb{Z}_d$, the cyclic group of order the degree d of the minimal polynomial of the extension $F \hookrightarrow F'$.*

Proof. Let $\mathbb{F}_p(t)$ be the rational function field of the projective line $\mathbb{P}^1(\mathbb{F}_p)$. One can consider towers $\mathbb{F}_p(t^{\frac{1}{d}})$ or $\overline{\mathbb{F}}_p(t^{\frac{1}{d}})$, as d varies through powers of the prime p or through all integers not divisible by the characteristic of the ground field, that is p . The corresponding field extension $F = \mathbb{F}_p(t) \hookrightarrow F' = \mathbb{F}_p(y)$, where y is a d -root of the polynomial $\sigma(t) = t^d - u \in \mathbb{F}_p(t)$ is a finite Galois extension of degree d . Moreover F'/F is an extension of Kummer type and \mathbb{F}_d is the full constant field. \square

Remark 2.3. *One of the main problems in coding theory is to obtain non-trivial lower bounds of the number $N(F_i)$ of rational places of towers of function fields $\{F_i/\mathbb{F}_q\}_{i=1}^{\infty}$ such that $F_i \subsetneq F_{i+1}$.*

Lemma 2.4. *Every Galois cover of the projective line, after a birational transformation can be written in the form*

$$y^n = \prod_{i=1}^s (x - \rho_i)^{d_i}, \quad d_i \in \mathbb{Z}.$$

Proof. By Lemma 2.2 any Galois cover of the projective line $\mathbb{P}^1(\mathbb{F}_p)$ corresponds to a finite field extension $F \hookrightarrow F(y)$ with y a d -root of the minimal polynomial $\sigma(t) = t^d - u \in \mathbb{F}_p(t)$. Let $S = \mathbb{P}^1(F) \setminus \{\text{poles and zeroes of } u \text{ in } F\}$. For any $P \in S$ we have that the polynomial $\bar{\sigma}_P(t) := t^d - u(P)$ factorizes in $\mathbb{F}_d[t]$ into pairwise distinct irreducible factors (see [CT]). \square

- Remark 2.5.** (1) *The covering ramifies exactly at the places $x = \rho_i$, and the corresponding ramification indices are defined by $e_i = \frac{n}{(n, d_i)}$, with d_i the corresponding multiplicity of ρ_i . If $d = \sum_{i=1}^s d_i \cong 0$, then the place at ∞ does not ramify at the above extension. The only places of F that ramify are the places P_i that correspond to the points $x = \rho_i$.*
- (2) *The genus of the function field F' can be computed with the aid of the Riemann-Hurwitz formula to be $g = \frac{(n-1)(s-2)}{2}$.*
- (3) *If $(n, d_1, \dots, d_s) = 1$, then F' is a Kummer extension of the rational function field F of order n .*
- (4) *The condition $(n, d_i) = 1$ is a stronger condition for all $i = 1, \dots, s$.*

Definition 2.6. *A curve \mathcal{C} is a p -cyclic cover of the projective line if and only if has a g_p^1 base point free linear system. If the linear system is unique, then the Galois cyclic group $\text{Gal}(\mathcal{C}/\mathbb{P}^1)$ is normal in G . A sufficient condition for g_p^1 to be unique is the inequality:*

$$2 \leq p \leq \frac{g}{2} + 1.$$

- Theorem 2.7.** (1) *We can determine all possible Galois coverings of the projective line by considering every finite subgroup of the projective linear group $PGL(2, q)$, the automorphism group of $\mathbb{P}^1(\mathbb{F}_q)$.*
- (2) *For each fixed degree d , the number of d -sheeted coverings $y^d = f_n(x)$ of $\mathbb{P}^1(\mathbb{F}_q)$ defined over \mathbb{F}_q is given by the sum $\sum_{k=1}^n (p)_k$, where $(p)_k$ is the falling factorial polynomial $q \cdot (q-1) \dots (q-(k-1))$, divided by the order of the affine transformation group of $\mathbb{A}^1 = \mathbb{P}^1 \setminus \infty$, that is $q^2 - q$.*

Proof. We observe that any Galois covering of the projective line $\mathbb{P}^1(\mathbb{F}_q)$ is given by a surjective morphism $\pi : \mathcal{Y} \rightarrow \mathbb{P}^1(\mathbb{F}_q)$, where \mathcal{Y} is a curve such that \mathcal{Y}/G is isomorphic to $\mathbb{P}^1(\mathbb{F}_q)$, being G a finite subgroup of $PGL(2, q)$ the automorphism group of the rational function field acting on $\mathbb{P}^1(\mathbb{F}_q)$ by:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : z \rightarrow \frac{az + b}{cz + d}, \quad A \in PGL(2, q).$$

If $G = PSL_2(q)$ (respectively, $PGL_2(q)$) with $q \leq 5$ (respectively, $q \leq 4$), then G is isomorphic to one of S_3, S_4, A_4 or A_5 . If $G = PSL_2(q)$ with $5 < q = p^e$, for some prime number p and some positive integer e , G is a quotient of a certain triangle group:

$$T_{r,s,t} = \langle x, y, z : x^r = y^s = z^t = xyz = 1 \rangle,$$

where r, s, t are integer numbers such that $\frac{1}{r} + \frac{1}{s} + \frac{1}{t} < 1$, the group $T_{r,s,t}$ is called a hyperbolic triangle group.

In order to prove the second part of the Theorem, we need to count all the polynomials $f_n(x)$ that define a d -sheeted covering of the projective line, by counting polynomials depending on the number of different roots.

Thus the number of separable polynomials of degree n over \mathbb{F}_q is q^n . The number of monic polynomials with $n - 1$ different roots is $q(q-1)(q-2)\dots(q-n+1)$, that is known as the falling factorial polynomial $(q)_n$ and it is the generating function for the signed Stirling numbers:¹

$$q_{(n)} = q(q-1)(q-2)\dots(q-n+1) = \sum_{k=0}^n s(n, k)q^k.$$

One can immediately see, that $(q)_1 = q$, because the number of polynomials with one different root is q , independently of the degree n of the polynomial $f(x)$. The number of polynomials with k different roots, where $1 \leq k \leq n$, is given by the falling factorial polynomial $(q)_{(k)}$.

Since only $\infty \in \mathbb{P}^1$ is distinguished, we must further divide by the group of affine transformations of $\mathbb{A}^1 = \mathbb{P}^1 \setminus \infty$. Since the order of the transformation group is $q^2 - q$, we have that the number of q curves over \mathbb{F}_q expressible as d -sheeted coverings of \mathbb{P}^1 is the falling factorial polynomial $(q-2)_n$. \square

Remark 2.8. *The case in which $\mathbb{P}^1(\mathbb{F}_q)$ is covered by a curve \mathcal{C} determined by a finite subgroup $G < PGL(2, q)$ such that the corresponding projection to the quotient surface $\mathcal{C} \rightarrow \mathcal{C}/G \cong \mathbb{P}^1(\mathbb{F}_q)$ is branched over 3 points plays an important role in the study of Beauville surfaces, (see [SG]).*

Remark 2.9. *Theorem 2.7 gives a motivation for the study of quotient curves arising from subgroups of $PSL(2, q)$ or $SL(2, q)$.*

2.1. The curve $y^m + x^n = 1$. Ihara showed that if a curve \mathcal{C} is maximal over \mathbb{F}_{q^2} , then

$$g(\mathcal{C}) \leq \frac{q(q-1)}{2}.$$

Up to \mathbb{F}_{q^2} -isomorphism, there is just one maximal curve over \mathbb{F}_{q^2} with this genus, the Hermitian curve \mathcal{H} which can be given by the equation $x^{q+1} + y^{q+1} + 1 = 0$. In this section we consider maximal curves $\mathcal{C}(n, m)$ given by the equation $y^m + x^n = 1$ over a finite field k of q^2 elements. Let us call by $F_{n, m}$ the function field $k(x, y)$ of the $\mathcal{C}(n, m)$, where $y^m + x^n = 1$ and let $G_{n, m}$ be its automorphism group.

Theorem 2.10. *(Kontogeorgis) The group $G_{n, m}$ is given as a central extension:*

$$1 \rightarrow \mu_m \rightarrow G_{n, m} \rightarrow D_m \rightarrow 1,$$

where D_m denotes the dihedral group of order $2n$. This extension splits if and only if m is odd. In this case, $F_{n, m} \cong \mu_m \times D_n$. In case $m|n$ and $n-1 = q$ is a power of the characteristic, the group of automorphisms is given as a central extension:

$$1 \rightarrow \mu_m \rightarrow G_{n, m} \rightarrow PGL(2, q) \rightarrow 1.$$

As in the previous case, this extension splits if and only if m is odd.

¹Stirling numbers of the second kind is the number of ways to partition a set of n objects into k non-empty subsets and is denoted by $s(n, k)$

In the case $n = q - 1$, the group of automorphisms $G_{n,m}$ surjects into the projective linear group $PGL(2, q)$. The curve is given by the equation $y^m = x^{q-1} + 1$. For any finite subgroup $G < PGL(2, q)$, we can consider the quotient curve $\mathcal{C}_{n,m}/G$.

Proposition 2.11. *For any element $A \in PGL(2, q)$, the function field of the quotient curve $\mathcal{C}_{q-1,m}/\langle A \rangle$ is the invariant field under the action of the group generated by A .*

Proof. Consider an element $A \in PSL(2, q)$ such that its characteristic polynomial $P(\lambda) = \lambda^2 - \alpha\lambda + 1$, where α is the trace of A has two distinct roots in \mathbb{F}_q , $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$, where $a \in \mathbb{F}_q^*$ and $a + a^{-1} = \alpha$. Let us call the group generated by the element $\langle A \rangle$ as G_1 . Then the function field of the quotient curve $\mathcal{C}_{n,m}/G_1$ is the invariant field under the action of $A \in PSL(2, q)$, so the automorphism of $k(x, y)$ with equation $A(x, y) = (ax, a^{-1}y)$. Then the subfield $k(x, y)^{G_1}$ consisting of all elements fixed by A is $k(\mu, \tau)$ where $\mu = x^{q-1}$ and $\tau = xy$.

Now we consider the element $B = \begin{pmatrix} a & 0 \\ 0 & a^q \end{pmatrix}$ in $PSL(2, q)$ with $a \in \mathbb{F}_{q^2}^* \setminus \mathbb{F}_q^*$ acting on $\mathbb{P}^1(\mathbb{F}_q)$ without fixed points. Then the function field of the quotient curve $\mathcal{C}_{n,m}/G_2$, where G_2 is the group generated by the element $B \in PGL(2, q)$, is the subfield $k(x, y)^{G_2} = k(\gamma, \delta)$, with $\gamma = x^{q^2-1}$ and $\delta = x^{-q}y$.

Finally, we consider any of the elements $C = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ acting on $\mathbb{P}^1(\mathbb{F}_q)$ with one fixed point by $C(x, y) = (x + y, y)$. If G_3 is the subgroup $\langle C \rangle$ generated by this element in $PGL(2, q)$, the quotient curve $\mathcal{C}_{n,m}/G_3$ is the invariant subfield by the action of the automorphism C . \square

Remark 2.12. *The points $P_0 = (\alpha, 0)$ and $P_1 = (\beta, 0)$ with $\alpha^m = 1$ and $\beta^n = 1$ are rational points of the curve $\mathcal{C}_{n,m}$ since $m|q^2 - 1$ and the root divisors of the elements $x, y \in k(x, y)$ are expressed as $\text{div}(y) = mP_0$ and $\text{div}(x) = nP_1$.*

REFERENCES

- [BM] A. Besana, C. Martínez, *Enumerative geometry of cyclic coverings of the projective line*, math.AG:1111.6456.
- [CT] M. Chara, R. Toledano, *Rational places in extensions and sequences of function fields of Kummer type*, Journal of Pure and Applied Algebra 215 (2011) 2603-2614.
- [SG] S. Garion, *On Beauville structures for $PSL_2(q)$* , matharXiv:1003.2792.
- [GT] M. Giulietti and F. Torres, *On dense sets related to plane algebraic curves*, Arcs. Combin. LXII (2004), 33-40.
- [Hirs] J. W. P. Hirschfeld, *Finite Projective Spaces of Three Dimensions*, Oxford Mathematical Monographs.
- [FP] C. Faber, R. Pandharipande, *Tautological and non-tautological cohomology of the moduli space of curves*, arXiv:1101.5489.
- [Kon] A. Kontogeorgis, *The group of automorphisms of the Function Fields of the Curve $x^n + y^m - 1 = 0$* , Journal of Number Theory 72, 110-136.

- [FGT] R. Furhmann, A. García, F. Torres, *On maximal curves*, Journal of Number Theory 67 (1) (1997), 29-51.
- [TT] S. Tafazolian, F. Torres, *On the characterization of certain maximal curves*, preprint.

DEPARTAMENT DE MATEMÀTIQUES, EDIFICI C, FACULTAD DE CIÈNCIES, UNIVERSITAT AUTÒNOMA DE BARCELONA, 08193 BELLATERRA, BARCELONA
E-mail address: `abesana@mat.uab.cat`

DIPARTIMENTO DI MATEMATICA "GUIDO CASTELNUOVO" SAPIENZA UNIVERSITÀ DI ROMA P.LE ALDO MORO, 5 - 00185 ROMA
E-mail address: `martinez@mat.uniroma1.it`
E-mail address: `cmartine@mat.uab.cat`